

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with the applicant's representative on 10/3/08.

The application has been amended as follows:

Listing of Claims:

1. (Currently Amended) A system for verification and installation of a virtual machine, comprising:

a processor:

a primary library file, the primary library file having a digital signature, wherein the primary library file is a virtual machine dynamic link library file;

a loader program that, when operated by the processor, checks for a public key from a virtual machine provider to use as a digital signature key and, if the digital signature of the primary library file is verified against the digital signature key, further loads the primary library file, wherein, if the public key cannot be obtained via the virtual machine provider, the digital signature key is a hidden public key internal to the loader program and, if the public key can be obtained via an internet site of the virtual machine provider, the digital signature key is the public key obtained via the virtual machine provider; and

a plurality of secondary files referenced by the primary library file, each of the plurality of secondary files having a digital signature;

wherein the loader program verifies and selectively loads the primary library file by comparing the obtained digital signature key with the digital signature of the primary library file, the primary library file subsequently verifying and selectively loading the plurality of secondary files by calling the loader program to compare the obtained digital signature key with the digital signature of each of the plurality of secondary files,

at least one tertiary file referenced by at least one secondary file of the plurality of secondary files, wherein after successful verification and selective loading of the at least one secondary file, the at least one secondary file manages the verification and selective loading of the at least one tertiary file,

at least one administrator-configurable file and

the digital signature key comprising a number of keys including a private key provided by an administrator,

wherein the loader program verifies the digital signature of the at least one administrator-configurable file using the private key, wherein the at least one administrator-configurable file includes at least one of a security file and a policy file that is updatable by use of the private key, wherein authenticity of each element of a virtual machine installation is verified.

2. (Cancelled).

3. (Cancelled).

4. (Cancelled).

5. (Cancelled).

6. (Cancelled).

7. (Currently Amended) A method for verification and installation of a virtual machine comprising:

launching a loader program operated by a processor and arranged to load library files;

checking for an availability of a public key from an internet site of a virtual machine provider;

if the public key is available from the internet site of the virtual machine provider, using the public key as a digital signature key;

if the public key is not available from the internet site of the virtual machine provider, using a hidden public key stored inside the loader program as the digital signature key;

using the loader program to verify authenticity of a digital signature incorporated in a primary library file by comparing said digital signature with the digital signature key, wherein the primary library file is a virtual machine dynamic link library file;

selectively loading the primary library file in dependence upon the successful verification of its digital signature;

for each of a plurality of secondary files, using the primary library file to verify authenticity of a digital signature incorporated in corresponding one of the plurality of secondary files by calling the loader program to compare the digital signature incorporated in the corresponding one of the plurality of secondary files with the digital signature key; and,

selectively loading the plurality of secondary files in dependence upon the successful verification of their digital signatures,

including at least one tertiary file referenced by at least one secondary file of the plurality of secondary files,

after successful verification and selective loading of the at least one secondary file, using the at least one secondary file to manage the verification and selective loading of the at least one tertiary file, at least one administrator-configurable file and

the digital signature key comprising a number of keys including a private key provided by an administrator,

wherein the loader program further verifies the digital signature of the at least one administrator-configurable file using the private key, wherein the at least one administrator-configurable file is loaded upon successful verification of any corresponding digital signatures, wherein the at least one administrator-configurable file includes at least one of a security file and a policy file that is updatable by use of the private key, wherein authenticity of each element of a virtual machine installation is verified.

8. (Cancelled).

9. (Cancelled).

10. (Cancelled).

11. (Cancelled).

12. (Cancelled).

13. (Cancelled).

14. (Previously Presented) The system for verification and installation of a virtual machine of claim 1, further characterised by: the virtual machine provider is accessed through an internet site to provide the public key.

15. (Previously Presented) The method for verification and installation of a virtual machine of claim 7, further characterised by: the virtual machine provider is accessed through an internet site to provide the public key.

16. (Cancelled).

17. (Cancelled).

18. (Previously Presented) The system for verification and installation of a virtual machine of claim 1, wherein the loader program is a third-party application that initiates the virtual machine installation.

19. (Previously Presented) The system for verification and installation of a virtual machine of claim 1, wherein the loader program is a virtual machine launcher that initiates the virtual machine installation.

20. (Previously Presented) The method for verification and installation of a virtual machine of claim 7, wherein the loader program is a third-party application that initiates the virtual machine installation.

21. (Previously Presented) The method for verification and installation of a virtual machine of claim 7, wherein the loader program is a virtual machine launcher that initiates the virtual machine installation.

22. (Currently Amended) A system for verification and installation of a virtual machine comprising:

a processor;

a virtual machine primary library file, the virtual machine primary library file having a digital signature;

a loader program that, when operated by the processor, checks for a public key from a virtual machine provider to use as a digital signature key and, if the digital signature of the primary library file is verified against the digital signature key, further loads the virtual machine dynamic link library file; and

a plurality of secondary files referenced by the virtual machine primary library file, each of the plurality of secondary files having a digital signature;

wherein the loader program verifies and selectively loads the virtual machine primary library file by comparing the obtained digital signature key with the digital signature of the virtual machine primary library file, the virtual machine primary library file subsequently verifying and, if the digital signature of the primary library file is verified against the digital signature key, loading the plurality of secondary files by calling the loader program to compare the obtained digital signature key with the digital signature of each of the plurality of secondary files, wherein, if the public key cannot be obtained via the virtual machine provider over the internet, the digital signature key is a hidden public key internal to the loader program and, if the public key can be obtained via an internet site of the virtual machine provider, the digital signature key is the public key obtained via the virtual machine provider over the internet;

at least one tertiary file referenced by at least one secondary file of the plurality of secondary files, wherein after successful verification and selective loading of the at least one secondary file, the at least one secondary file manages the verification and selective loading of the at least one tertiary file; at least one administrator-configurable file; and the digital signature key comprising a number of keys including a private key provided by an administrator,

wherein the loader program verifies the digital signature of the at least one administrator-configurable file using the private key, wherein the at least one administrator-configurable file

includes at least one of a security file and a policy file that is updatable by use of the private key, wherein authenticity of each element of a virtual machine installation is verified.

23. (Cancelled).

24. (Cancelled).

25. (Cancelled).

26. (Cancelled).

27. (Previously Presented) The system for verification and installation of a virtual machine of claim 18, wherein the third-party application launches the loader program through a native interface.

28. (Previously Presented) The method for verification and installation of a virtual machine of claim 20, wherein the third-party application launches the loader program through a native interface.

29. (Previously Presented) The system for verification and installation of a virtual machine of claim 27, wherein a binary module is linked into the third-party application and performs verification.

30. (Previously Presented) The method for verification and installation of a virtual machine of claim 28, further comprising linking a binary module into the third-party application, the binary module performing verification.

The following is an examiner's statement of reasons for allowance:

The prior art enables for a system to verify the authenticity of software installation, including the provision of a loader program and a plurality of secondary and tertiary files that verified and selectively loaded. However, the prior art does not appear to disclose the claimed features (e.g. *a loader program that, when operated by the processor, checks for a public key from a virtual machine provider to use as a digital signature key and, if the digital signature of the primary library file is verified against the digital signature key, further loads the primary library file, wherein, if the public key cannot be obtained via the virtual machine provider, the digital signature key is a hidden public key internal to the loader program and, if the public key can be obtained via an internet site of the virtual machine provider, the digital signature key is the public key obtained via the virtual machine provider*) as they are found recited in combination within claim 1 and similarly recited within claims 7 and 22.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFERY WILLIAMS whose telephone number is (571)272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J. W./
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437